www.einvestigations.com
(800) 713-7670

Digital Debugging: What is Spyware and How is it Detected and Prevented?

March 22, 2012

Summary:

This paper explores the complexities of digital bugs, also known as spyware and malware. With so much data stored on computers, laptops, smart phones and tablets, these devices are often targeted for cyber attacks. The spyware may harvest confidential and sensitive information by providing the perpetrator with remote access through the internet. Or malware may disrupt the function of the device or even an entire network causing damage and financial loss. Digital debugging involves not only detecting and documenting the bug and attempting to seek out its origin, but also installing preventative measures to stop the bug.

Copyright © 2012 McCann EI

Physical and digital bugging

If one heard the phrase "my phone is bugged" ten or fifteen years ago, the first image that would come to mind would be a scene from some 1980s movie in which the main character discovers a recording device attached to his landline phone socket. However, while the current reality is much less dramatic, the potential consequences have become much more dangerous. Within today's rapidly changing world of technology, the spyware sector has shown one of the fastest development rates. Although we no longer need to fear physical bugs, we must focus our attention on scanning for digital ones. The latter have a number of important competitive advantages over the former. While physical bugs, such a chips or recording devices, need to be physically planted at the location at a heightened risk of exposure for the criminal, the digital bug can be installed remotely and can target any electronic device. Smartphones are usually protected against remote installations, meaning that the criminal must have physical possession to install the bug directly into the device. However, in the hands of a professional, the whole procedure may take as little as 10-15 minutes. Also, the field of smartphone bugging will undoubtedly evolve in the near future to allow for remote installations.

Characteristics of spyware

So what is spyware and what can it do? Spyware is a type of malware (malicious software) installed on computers or other electronic devices that collects information about users without their knowledge. One common type of spyware is keyloggers (keystroke loggers), which track the keys struck on a keyboard and are particularly effective for collecting logins and passwords. Other spyware programs can harvest and transmit screenshots, clipboard content, documents, web history, emails, text messages and financial information. They can be installed on all types of computers - laptops, desktops, servers, and smartphones. Most programs harvest the information and then transmit it over the Internet to be remotely stored. However, other bugs may allow the perpetrator to remotely access in real-time the data from your electronic device. With

Copyright © 2012 McCann EI

the prevalence of personal computers and phones in our lives, having full access to the digital information that is being created or exchanged enables the criminal to harm you, financially or otherwise.

Reasons for bugging

But why would your phone or computer get bugged? You may be the target of a premeditated act in which somebody intentionally installs a bug onto your computer or smartphone with the aim of monitoring you. It may be your spouse or ex-spouse, boss, business competitor, etc. Additionally, it is also really easy to randomly pick up spyware while surfing the net. In addition to other malware such as viruses or Trojans, spyware can be picked up by downloading the wrong file, clicking on the wrong banner, visiting the wrong site or even simply by being connected to the Internet without using a firewall (the malware can be installed through vulnerabilities in one of your programs).

In case you are wondering why anybody would want to install spyware on random computers all over the world, consider the case of Jason Maybrick, a project manager of an energy research company in Houston. He left his office at 5pm and by the time he returned back to work at 9am he discovered that several hundred blueprints and research results had been approved and downloaded from his account in less than 24 hours. He immediately alerted his boss and changed the login and password to his account. Suspecting an inner fraud, his company contacted McCann E-Investigations at once and called for an expert to examine Jason's computer. After finding nothing suspicious on his work computer, the investigator asked if Jason had been accessing his account from his home computer, and it turned out that he had. On his home laptop a powerful keylogger was found, which was harvesting all of the information Jason had been typing in, including his work account login and password. Jason's laptop was completely scanned by the forensics experts with the help of complex anti-virus software, and then it was equipped with a new firewall to prevent any further attacks. Later in the investigation, it was discovered that the files were stolen by Chinese IP addresses from the other side of the world. The penetrators could have had no

Copyright © 2012 McCann EI

information about Jason's home computer, and yet were able to monitor his actions on it. Criminal companies like these simply collect information from millions of users who happen to accidentally pick up their bug to digitally scan the harvested data for lucrative opportunities. Like Jason, you can unwittingly become just another victim of the flourishing industry of cyber crime.

Cyber crime as a unique crime model

The worldwide boom of cyber crime can be explained by its unique capabilities. For the first time in history, crime occurs instantaneously, often without the victim even realizing that it has happened, and it can continue for a long time before the victim realized that they have been targeted. This type of crime can be committed from far away, from the other side of the globe in many cases, so there is often no need for direct contact. Furthermore, cyber crime is easy to hide and difficult to track. A good hacker will use a network of proxy servers to collect the necessary data piece by piece. Even if the source is found, it is often exceptionally problematic to pin the blame on a particular individual or company. The perpetrator may maintain they were unaware of the attack and that they were themselves the victim of malicious software installed onto their computer without their knowledge. Therefore, this type of crime carries very low risk. At the same time, the ROI (return on investment) is extremely high. A hacker only needs to create penetrative malware that installs itself on multiple computers, successfully exploiting the varying vulnerabilities in each of them. After the network is created, it can be used for various purposes, such as DDoS (distributed denial-of-service) attacks, collecting information, or spreading the malware even further. The advantage of cybercrime is that it is automated and strikes multiple targets at once. Thus, the returns can often reach hundreds of thousands of dollars a day.

As a response to cyber crime, the cyber security industry has grown rapidly since the 1990s and has introduced measures such as anti-virus software, firewalls (software of devices that protect your computer form unauthorized attacks and scans), data

Copyright © 2012 McCann EI

encryption, etc. Since the industry's inception, it has been in a constant battle with cyber crime, with both sides constantly escalating and refining their methods, while looking for ways to evade and advance over the other. This battle is likely to continue for as long as we use Internet-enabled electronic devices, so we better be aware of the possible risks.

Signs of bugging

A telling sign that your computer or phone is bugged is through not digital clues but instead personal ones: competitors have inside information about your business plans, products, etc. that have not been made public, a spouse has information they could not possibly know, or your private information has become available on the Internet. To make sure that this leak is caused by spyware as opposed to a personal disclosure, check for the information or activity flowing from your computer of smartphone. A telling sign that information from you device is being transmitted somewhere else is if the outgoing traffic exceeds the incoming one and you know you have not been uploading anything. For the majority of Internet users, the incoming traffic surpasses the outgoing one by several times. Other signs of bugging can include an increased CPU (central processing unit) load when there is no obvious activity on the computer or noise from your hard drive even when you are not actively using the computer. If your phone is bugged, it will likely create a constant clicking background noise when held near audio speakers. Other hints are if the screen accidentally lights up when you are not using it or if you notice some other strange activity of your device. Finally, the battery life is a good indicator of phone activity. If your phone is warm even when not in use or if it loses charge more quickly than it should, you may be a victim of spyware activity. However, it may be just a bad battery, so instead of jumping to hasty conclusions, take the steps to check your phone for spyware.

Copyright © 2012 McCann EI

Debugging methods

First of all, it is a good idea to update your anti-virus program and to scan all of the drives for possible malware. You can also buy software that is specifically geared towards spyware detection. The weaknesses of this software are that it is only as good as the last update and that finding the bug is not 100% guaranteed. Moreover, a skilled hacker can bypass the firewalls and anti-spyware programs. However, it is still advisable to not ignore the basics of computer security and to have a working updated anti-virus system at all times.

If your anti-virus program does not find anything suspicious, but you still feel that you are being monitored, post some false information as a test and see if it leaks out. The exposure of this information is a strong signal of a legitimate breach. At this point, you have two options – to buy more security scan software or to hire a forensic expert. Store-bought security scans examine firewalls, perform penetration testing, locate, minimize and plug holes in the security system. However, locating the source of penetration for a non-professional is an exceptionally challenging undertaking, so the likelihood of the culprit being found is low. Even if you succeed in tracking down the hacker responsible, the manner of discovering the information will make it unusable in court. For the data to be valid, they need to be collected by an independent third party, ideally by a professional in digital forensics.

If the breach is external, which means that your computer was hacked from an outside source unrelated to your company or social circle, it is usually very difficult to obtain proof or documentation due to the remote nature of the installation. However, in the case of an internal breach in which the spyware is installed by an employee, a family member, etc., it is possible to obtain proof with the proper resources and tools.

Copyright © 2012 McCann EI

Debugging with digital forensics

One of the leaders in the digital forensics field, McCann E-Investigations, utilizes two of the industry's most respected tools, QualysGuard and Nessus Security Scanners, as well as proprietary software, to identify and remediate security threats. The QualysGuard scanner is driven by the most comprehensive and up-to-date knowledge of vulnerability checks in the industry. QualysGuard delivers continuous protection against the latest worms and security threats. In performing over 150 million system audits per year, QualysGuard is the widest deployed on-demand security solution in the world. The Nessus Security Scanner detects and identifies the most malicious types of malware, such as spyware and keyloggers, which can capture and transmit confidential session data. The Nessus Security Scanner allows the computer forensics professionals to perform sophisticated remote scans and audits of Unix, Windows, and network infrastructures.

A different set of technology is used with mobile phones, which allow the digital forensic experts to interface directly with the phone and to look at it at a much deeper level than at just the visible apps. The mobile forensics technicians use several tools including the Cellebrite UFED Physical Pro forensic phone analyzer and Paraben Device Seizure and BitPim to connect to and query mobile phones, obtain and download file system dumps, and perform full physical phone images. The digital forensic experts then use the information obtained and imaged from the phone to search it against their database of mobile phone spyware utilities, tracking apps, and monitoring programs.

However, clearing the bug is only the first step of the debugging process. The second step is analyzing existing security systems such as firewalls, anti-virus programs and policies and procedures. Implementing new technologies, software and polices is the third step, so that you can be up-to-date in the affordable technology designed to keep your data and communications secure. The final step is constantly monitoring, updating and testing the solutions implemented. A digital forensic expert offers all of these solutions for your and your company's best protection.

Copyright © 2012 McCann EI